DEPARTMENT OF SOCIAL SERVICES
744 P Street, Sacramento, California 95814

March 6, 2000

REASON FOR THIS TRANSMITTAL

[ ] State Law Change
[ ] Federal Law or Regulation Change
[ ] Court Order
[x] Clarification Requested by One or More Counties

ALL-COUNTY INFORMATION NOTICE I-23-00

TO: ALL COUNTY WELFARE DIRECTORS
ALL COUNTY FISCAL OFFICERS
ALL COUNTY INCOME AND ELIGIBILITY VERIFICATION SYSTEM COORDINATORS

SUBJECT: INTERNAL REVENUE SERVICE SAFEGUARD REQUIREMENTS

REFERENCE: INTERNAL REVENUE CODE SECTIONS 6103(1)(7) AND 6103(P)(4); PUBLICATION 1075, TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE AND LOCAL AGENCIES

The purpose of this letter is to provide counties with instructions regarding the Internal Revenue Service (IRS) safeguard requirements for handling the Federal tax data. This data is included in the IRS Asset Match abstracts and the Beneficiary Earnings Exchange Record (BEER) match abstracts. Recently, the California Department of Social Services' (CDSS) IRS safeguard procedures were reviewed by IRS staff to determine whether California is in compliance with Federal law. As a result of this Federal review, CDSS is providing counties with instructions to clarify how counties should be handling IRS tax data in receiving, processing, storing and destroying IRS Asset and BEER rosters and abstracts.

BACKGROUND

California uses the Income and Eligibility Verification System (IEVS) to determine eligibility and identify overpayments and fraud in the California Work Opportunity and Responsibility to Kids and Food Stamp Programs. This includes obtaining and utilizing Federal tax data from the IRS and Social Security Administration. Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies states that, as a condition for receiving the Federal tax data, State welfare agencies must establish and maintain certain safeguards designed to prevent unauthorized uses of the tax information and to protect the confidentiality of that information.

A Federal safeguard review of CDSS was conducted in December 1998. This review included on-site visits to two counties to determine how counties are following federal safeguard requirements. In addition, Fraud Bureau staff conduct reviews of county IEVS operations, which includes a determination of whether the county is in compliance with Federal IRS safeguard requirements. CDSS shares the results of these reviews

with the IRS as a means of monitoring county compliance with IRS safeguard requirements. Results of these reviews indicate that there is a need for clarification of how counties can meet IRS safeguard requirements. Therefore, CDSS is issuing these reminders regarding how counties should be handling, storing and destroying IRS Asset and BEER tax data. In accordance with Publication 1075 and Division 19 of the CDSS Manual of Policies and Procedures the following security conditions must be met:

STORAGE – PHYSICAL SECURITY OF FEDERAL TAX DATA

- Federal tax data must be stored in a locked cabinet in a locked room. The key to the locked cabinet must be placed in a locked container, such as a desk drawer, or kept with an authorized employee at all times.

- If the room where Federal tax data is stored cannot be locked or if the room contains a window and is located on the first floor, the room must be equipped with an electronic intrusion detection device. This includes, but is not limited to, window contacts, magnetic switches, motion detectors and sound detectors that set off an alarm at a given location when the sensor is disturbed. Alarms must be connected to an on-site protection console or a local/central police station.

- If electronic intrusion devices are not a viable solution, security glass can be installed on the window. Door hinge pins must be non-removable or installed on the inside of the room. The room must be enclosed by slab-to-slab walls (there should be no space between the top of the wall and the ceiling).

- The space where Federal tax data is stored must be cleaned during business hours or in the presence of a regularly assigned employee.

- Access to any locked area or container can only be controlled if the keys are properly controlled. Logs must be maintained to show employee key assignment and periodic inventories of those keys conducted. In addition, there must be a notation on all keys stating that they are not to be duplicated.

RESTRICTING ACCESS TO FEDERAL TAX DATA

- If Federal tax data (name and address of the payer and account numbers) is included in a verification letter, case history or subpoena, the Federal tax data never

loses its character as Federal tax data. This holds true even if a third party verifies the information. Therefore, if tax data is placed inside a case file, the entire file must be protected and access restricted to authorized agency personnel.

- As an alternative to locking up the entire case file, the Federal tax data can be placed in a separate file or folder and not placed in the case file. This separate file can then be locked in a secure area.

- Due to the confidential nature of the Federal tax data, county worker notes cannot be entered into the Statewide Automated Welfare System (SAWS) or any other computer database, unless computer security meets Federal requirements as outlined in Publication 1075. Documentation in SAWS must be limited to generic references such as "IRS Asset match processed on June 10, 1999; no discrepancy." Detailed notes on any findings can be made on the abstract.

- Envelopes containing IEVS reports/abstracts must be stored securely as soon as the county receives the Federal tax data. These envelopes cannot be left on the IEVS Coordinator's desk unless the IEVS Coordinator is present. When the IEVS Coordinator is absent, the envelopes must be stored in a secure location, i.e., in a locked cabinet within a locked room.

- Counties must notify county employees utilizing the Federal tax data of the penalties associated with unauthorized access of Federal tax data. This shall be done on an annual basis through memos or group meetings.

- County employees accessing Federal tax data shall be made aware of the civil and criminal penalties for unauthorized access, and/or inspection or disclosure of Federal tax information to unauthorized individuals.

DISPOSAL OF FEDERAL TAX DATA

- Counties must establish a policy for disposing of information containing Federal tax information. The disposal process must be completed or monitored by an agency employee to prevent unauthorized access. In addition, a log must be maintained to record the particular material being destroyed, along with the date and manner of destruction. Federal tax information, including any related notes and work papers,

must be destroyed by burning, mulching, pulping, shredding or disintegrating. When shredding Federal tax data, the counties must use a cross shredder to meet the Federal requirement of 5/16-inch wide or smaller strips.

- If the county chooses to store old Federal tax data rather than destroy it, storage facilities must meet the requirements described above.

If you would like a copy of Publication 1075 or have any questions regarding this letter, please call Kelli Yasumura of the Fraud Bureau at (916) 263-5718.

Sincerely,

Original Document Signed by
Calvin Rogers on 3/6/00

CALVIN ROGERS, Chief
Program Integrity Branch